REMARKS

Upon entry of this amendment, claims 1, 3-18, 20-26, 28-29, 31, and 46-50 will be pending. By this amendment, claims 1, 10, 18, 26, 29, and 46 have been amended. No new matter has been added.

Response to the Examiner's comments about Information Disclosure Statement

In Section 3 of the Office Action, the Examiner states that "[a]n applicant's arguments filed with respect to the Information Disclosure Statement have been fully considered but they are not persuasive. In view of the vase number of references cited in the case, in addition to the new information disclosure statements filed since the last outstanding Office Action, Examiner maintains the position that by initialing each of the cited references on the accompanying 1449 forms, the examiner is merely acknowledging the submission of the cited references and merely indicating that only a cursory review is made of the cited references.'"

Applicants would like to state for the record that C.F.R. §1.56 (Duty to disclose information material to patentability) states that "[e]ach individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned."

Further, C.F.R. §1.97(b)-(d) states that an "information disclosure statement shall be considered by the Office if filed by the applicant within" certain "time periods."

§102 Rejection of Claims 1, 3-6, 8, 9, 18, 20-21, 26, 28-29 and 46-49

In Section 7 of the Office Action, claims 1, 3-6, 8, 9, 18, 20-21, 26, 28-29 and 46-49 stand rejected under 35 U.S.C. 102(e) as being anticipated by Steenkamp *et al.* (U.S. Patent Publication No. 2004/0168184; hereinafter referred to as "Steenkamp").

Regarding amended claim 1, it recites:

> A method of adding a client as a member of a hub network, comprising:
>
> (a) detecting a client connected to a server in a hub network;
>
> (b) authenticating said client;
>
> (c) authorizing said client; and
>
> (d) adding said client as a member in said hub network,
>
> (e) wherein the server provides a license for content data bound to the hub network to all members of the hub network.
>
> (emphasis / limitation designations added)

In addition to the arguments presented in responses to previous office actions (which are maintained here), following additional arguments are presented.

Regarding limitation (e) of claim 1, it recites "wherein the server provides a license for content data bound to the hub network to all members of the hub network". This limitation is disclosed in at least Paragraph [0061] (of the Publication of the present invention – Pub. No. 2004/0117484) as follows (emphasis added):

> [0061] The server for a hub network is the focal point of the hub network and manages many aspects of the control of the hub network. A server manages root responsibility for bound instances of content and provides the content to client members in the hub network. A server stores the source version of the locked content data and the corresponding root license of a bound instance. A server provides a sub-copy version of locked content data for a bound instance to a client or streams data of a source version of locked content data to a client. A server manages instances, handles licensing, administers network membership, monitors connection and disconnection of devices to the hub network, and performs time administration. A server defines the local environment of the hub network. As discussed below, a server binds instances of content to a hub network by shifting the state of an instance from discrete (external to the hub network) to bound (internal to the hub network), and a server frees instances from a hub network by shifting the state of an instance from bound to discrete.

Therefore, the server grants licenses for content data bound to the hub network to all members of the hub network.

In addressing limitation (e) of claim 1, the Office Action indicates that it is disclosed in Steenkamp, Paragraphs 68, 98, and 102, where "licenses are granted (issued) only to clients who have been added as members (subscribers) of the digital rights network. These paragraphs of Steenkamp are recited here for reference (emphasis added):

> [0068] To review, the content distribution system 10 is implemented by a distributed collection of digital rights servers 36, digital rights agents 28, and digital rights clients 48 that operate in conjunction with media servers and viewing devices (e.g., players) to protected the rights of a content provider 16 in specific content, while facilitating the widespread distribution of content. A digital rights server 36 enables the content provider 16 to encrypt and associate access criteria (e.g., pay-per-view, pay-per-time,

> subscription) with content. The digital rights server 36 also manages subscriptions and provides monitoring and statistic tools to a content provider 16. A digital rights agent 28 is a cryptographic component that insures that content rights (e.g., access criteria), as defined by content providers 16, are enforced. Digital rights agents 28 are located within a distribution network (e.g., at an edge server) and validate subscriber content requests against, for example, content access criteria, local date and time, and subscriber credentials. A digital rights client 48 is located at a destination device (e.g., the PC, a STB, and mobile phone, game console or the like) and manages an interface between a secure device 46 and a subscriber.
>
> [0098] A digital rights agent 28 also operates to create licenses for distribution to a content destination 22 so as to allow a content consumer to access specific content. Licenses for content may be created within the digital rights agent 28 utilizing a variety of license formats, based on the relevant user secure media player 46. In some cases, content may be delivered in the clear, but access to the content limited through a simple access control (i.e., content is not delivered from a content distributor 20 until user rights of a content consumer to access the content have been cleared).
>
> [0102] The content destination 22 (e.g., a secure device 46 operated by a content consumer) is shown to request and receive licenses from a digital rights agent 28. In one embodiment, the digital rights agent 28 issues a license on behalf of a content rights owner (e.g., a content provider 16), and a commerce service provider 42 (e.g., a CRM operator) for a content consumer. The license is issued if an access policy associated with the requested content is satisfied, and the content consumer's account is in order. Such a license typically contains a content decryption key, and certain rules governing the use of the decryption key. The content destination 22 is also shown to receive content from the content distributor 20, this content typically being encrypted and requiring the above-mentioned content decryption key for access.

However, applicants respectfully disagree with the Examiner regarding the

characterization of limitation (e) of claim 1 as being disclosed by Steenkamp. In particular, paragraph [0069] states that a "digital rights agent 28 also operates to create licenses for distribution to a content destination 22 so as to allow a content consumer to access specific content. Licenses for content may be created within the digital rights agent 28 utilizing a variety of license formats, based on the relevant user secure media player 46. In some cases, content may be delivered in the clear, but access to the content limited through a simple access control (i.e., content is not delivered from a content distributor 20 until user rights of a content consumer to access the content have been cleared)." Therefore, it is clear that the Steenkamp's digital rights network does not provide for granting licenses for content data bound to the hub network to all members of the hub network. Steenkamp does not suggest granting licenses for all "bound" content data, where the term "bound" indicates that the content data is available to members connected to (or bound to) the hub network. In contrast, limitation (e) of claim 1 discloses that licenses are granted for content data bound to the hub network to all members of the hub network, which suggests that licenses for content data is granted for all members bound to the network regardless of status.

Based on the foregoing discussion, claim 1 should be allowable over Steenkamp. Regarding independent claims 18, 26, 29, and 46, similar arguments as those of claim 1 apply to these claims. Therefore, claims 18, 26, 29, and 46 should also be allowable over Steenkamp. Since claims 3-6, 8, 9, 20-21, 28 and 47-49 depend from one of claims 18, 26, and 46, claims 3-6, 8, 9, 20-21, 28 and 47-49 should also be allowable over Steenkamp. Claims 2, 19, 27, and 30 have been canceled.

Accordingly, it is submitted that the rejection of claims 1-6, 8, 9, 18-21, 26-30 and 46-49 based upon 35 U.S.C. §102(e) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 7 and 22

In Section 25 of the Office Action, claims 7 and 22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 1 and 18 above, and further in view of Kamperman (U.S. Patent Publication No. 2005/0273608).

Regarding claims 7 and 22, they recite "authenticating said client includes sending a compliance confirmation request to said client, said compliance confirmation request requests information from said client to confirm that said client is a compliant device, and a compliant device will not decrypt locked content data without a license that is bound to a hub network of which the compliant device is a member" (claim 7) and "sending compliance information from said client to said server; wherein said compliance information indicates that said client is a compliant device, and a compliant device will not decrypt locked content data without a license that is bound to a hub network of which the compliant device is a member." (claim 22) These limitations are disclosed in at least Paragraph [0079] (of the Publication of the present invention – Pub. No. 2004/0117484) as follows (emphasis added):

> [0079] The server authenticates the detected client device, block 1815. The server sends a compliance confirmation request for information from the client device to establish whether the client device is a compliant device or not. For example, the server sends a confirmation request encrypted for a compliant device. If the client device does not respond properly or the server otherwise

> determines that the client device is not a compliant device, the authentication fails and the server will not add the client device as a member to the hub network.

In addressing claims 7 and 22, the Office Action indicates that Paragraphs [0005] to [0006] and [0029] to [0031] of Kamperman disclose the limitations of claims 7 and 22. These paragraphs are recited here for reference (emphasis added):

> [0005] One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if
>
> [0006] the receiving device has been authenticated as being a compliant device,
>
> [0029] In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,
>
> [0030] performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is compliant with a set of predefined compliance rules,
>
> [0031] if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device.

Although the above-cited passages recite authenticating the receiving device as being compliant device, they fail to disclose "sending a compliance confirmation request to said client, said compliance confirmation request requests information from said client to confirm that said client is a compliant device, and a compliant device will not decrypt locked content data without a license that is bound to a hub network of which the compliant device is a member." Specifically, none of the paragraphs disclose that the compliant device will not decrypt locked content data without a license that is bound to a

hub network of which the compliant device is a member.

Based on the foregoing discussion, claims 7 and 22 should also be allowable over Steenkamp and Kamperman.

Accordingly, it is submitted that the rejection of claims 7 and 22 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 10, 23, 28, and 31

In Section 28 of the Office Action, claims 10, 23, 28, and 31 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 9, 18, 26, and 29 above, and further in view of Fransdonk (U.S. Patent Publication No. 2003/0167392).

Regarding claim 10, it recites "said local environment confirmation request requests information from said client indicating whether said client in a local environment of said server, and said local environment is a limited area defined relative to said server." This limitation is disclosed in at least Paragraph [0082] (of the Publication of the present invention – Pub. No. 2004/0117484) as follows (emphasis added):

> [0082] After receiving a request to add the client device, the server authorizes the client device, block 1825. In one implementation, the client must be in the local environment of the hub network to be added. The server sends a local environment confirmation request for information from the client to establish whether the client device is in the local environment of the hub network. In one implementation, the server sends a test message and waits for a response from the client (e.g., pings the client). Based on the

> amount of time between sending the test message and receiving the response, the server determines whether the client is in the local environment (e.g., a round trip time below a threshold indicates a client is within the local environment). In another implementation, the server sends local environment information to the client device and the client device determines whether the client device is in the local environment or not. If the server does not establish that the client device is in the local environment of the hub network, the authorization fails and the server will not add the client device as a member to the hub network.

In addressing claim 10, the Office Action indicates that Paragraphs [0368] to [0371] of Fransdonk discloses the limitation of claim 10. These paragraphs are recited here for reference (emphasis added):

> [0368] It is desirable to provide a content provider 16 with geographic control over the distribution of content for a number of reasons. For example, a content provider 16 may wish to distribute a live event over the Internet worldwide, but need to block certain countries (e.g., or reasons due to exclusive broadcasting rights having been sold to broadcasters in those regions). According to one aspect of the present invention, there is provided a method and system to provide content providers 16 with secure geographic distribution control.
>
> [0369] At a high level, the present invention proposes that content providers 16 encrypt content before distribution of a network (e.g., the Internet). In order to view the encrypted content, a content destination 22 will need to retrieve the encrypted content and the associated encryption key (or keys). Prior to communicating such encryption keys and content, according to one aspect of the present invention, a user and/or a copy-protected device are authenticated with secure hardware devices (e.g., PKI-enabled hardware devices such as smart cards or USB e Tokens). Once a user or copy-protected device has been identified, a number of geographic location checks are then performed against geographic access criteria to determine whether or not to release content to a requesting content destination 22.
>
> [0370] FIG. 24 is a flowchart illustrating a method 550,

> according to an exemplary embodiment of the present invention, of distributing content via a network (e.g., the Internet) in a geographically controlled manner. The method 550 commences at block 552 with the receipt of a request from a content requestor located at a content destination 22 for delivery of content via a network to the content destination 22. The request may, for example, be received at conditional access agent 28, as illustrated in FIG. 2 from a conditional access client 48, located at the content destination 22. As described above with reference to Figure 16, the request to the conditional access agent 18 may include both a user authentication device certificate 404 and a copy-protected device certificate 410.
>
> [0371] At block 554, the conditional access agent 28, in the manner described above, retrieves access criteria associated with the request content from an appropriate conditional access server 36 operated via a content provider 16, or by a service provider 38. The retrieved access criteria includes geographic access criteria specifying geographic regions (e.g., countries, states, provinces, counties, towns, municipal areas, etc.) and access conditions associated with those geographic regions. For example, the geographic access criteria may prohibit, or alternatively authorize, distribution of the associated content to a specific geographic region or regions. For the purposes of the present specification the term "geographic location" shall be taken to include any geographic location identifiable by any criteria, including national, state, municipal, city, town, economic, demographic, historical, or a socio-economic criteria.

However, applicants respectfully disagree with the Examiner regarding the characterization of the limitation of claim 10 as being disclosed by Fransdonk. In fact, fransdonk merely discloses providing "geographic control over the distribution of content" rather than sending a local environment confirmation request for information from the client to establish whether the client device is in the local environment of the hub network so that the client can be added to the hub network.

Based on the foregoing discussion regarding claim 10, claim 10 should be allowable over the combination of Steenkamp and Fransdonk. Based on the foregoing discussion regarding claims 18, 26, and 29, and since claims 23, 28, and 31 depend from claims 18, 26, and 29, respectively, claims 23, 28, and 31 should also be allowable over Steenkamp. Fransdonk was cited merely for disclosing the limitations of claims 23, 28, and 31. Without admitting that Fransdonk does in fact discloses the above-recited limitations, it is submitted that the combination of Steenkamp and Fransdonk still fails to disclose all limitations of claims 23, 28, and 31.

Accordingly, it is submitted that the rejection of claims 10, 23, 28, and 31 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 11, 12 and 50

In Section 33 of the Office Action, claims 11, 12 and 50 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 9 and 49 above, and further in view of Uhlik (U.S. Patent Publication No. 2007/0112948).

Based on the foregoing discussion regarding claims 1 and 46, and since claims 11-12 and 50 depend from claims 1 and 46, respectively, claims 11, 12, and 50 should also be allowable over Steenkamp. Uhlik was cited merely for disclosing the limitations of claims 11, 12, and 50. Without admitting that Uhlik does in fact discloses the above-recited limitations, it is submitted that the combination of Steenkamp and Uhlik still fails to disclose all limitations of claims 11, 12, and 50 (because of added limitations to claim

1).

Accordingly, it is submitted that the rejection of claims 11, 12 and 50 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 13 and 25

In Section 39 of the Office Action, claims 13 and 25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 1 and 18 above, and further in view of McCann *et al.* (U.S. Patent No. 7,376,840; hereinafter referred to as "McCann").

Based on the foregoing discussion regarding claims 1 and 18, and since claims 13 and 25 depend from claims 1 and 18, respectively, claims 13 and 25 should also be allowable over Steenkamp. McCann was cited merely for disclosing: checking a revocation list to determine whether said client is included in said revocation list, wherein said revocation list is stored on said server (claim 13); and checking a revocation list to determine whether said client is included in said revocation list, wherein said revocation list is stored on said client (claim 25). Without admitting that McCann does in fact discloses the above-recited limitations, it is submitted that the combination of Steenkamp and McCann still fails to disclose all limitations of claims 13 and 25 (because of added limitations to claim 1).

Accordingly, it is submitted that the rejection of claims 13 and 25 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is

respectfully requested.

§103 Rejection of Claims 14-17

In Section 42 of the Office Action, claims 14-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claim 1 above, and further in view of Abburi *et al.* (U.S. Patent No. 7,203,966; hereinafter referred to as "Abburi").

Based on the foregoing discussion regarding claim 1, and since claims 14-17 depend from claim 1, claims 14-17 should also be allowable over Steenkamp. Abburi was cited merely for disclosing the limitations of claims 14-17. Without admitting that Abburi does in fact discloses the above-recited limitations, it is submitted that the combination of Steenkamp and Abburi still fails to disclose all limitations of claims 14-17 (because of added limitations to claim 1).

Accordingly, it is submitted that the rejection of claims 14-17 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

Conclusion

In view of the foregoing, applicants respectfully request reconsideration of claims 1, 3-18, 20-26, 28-29, 31, and 46-50 in view of the remarks and submit that all pending claims are presently in condition for allowance.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number written below.

Respectfully submitted,

Dated: 3-25-10

By: _____
Samuel S. Lee
Reg. No. 42,791

Procopio, Cory, Hargreaves & Savitch LLP
530 B Street, Suite 2100
San Diego, California 92101-4469
(619) 525-3821